Dr. Ernest McDuffie

“National Initiative for Cybersecurity Education”

CyberFutures Conference
National Harbor, Maryland
1 April 2011

Dr. McDuffie: Thank you very much for this opportunity. I really appreciate the opportunity to be here this afternoon and speak to this group.

I spent nine years in the Air Force as an enlisted person. It’s really good to be back home with the Air Force. Some of my most enjoyable experiences were at Fort Meade, part of the security service up there. So I’m really glad to be back and talk to this group.

Just listening to the previous speaker, I feel like I’m already talking to the choir. You guys understand exactly what’s happening in cyberspace, how important the training and education piece is. The people component of cyberspace is really the critical component now that we’re starting to focus on.

I’m going to give you a little background on what the NICE Initiative is all about and walk us through where we are right now with that and where we’re going to be going in the future.

I’m sure most of you are familiar with the CNCI, the Comprehensive National Initiative for Cybersecurity which was stood up under the previous administration. That program was federally focused, was looking internal at the federal government, workforce and issues there. When the new administration came on-board, they looked at that program and said there were really good things happening in that space. So good, in fact, that they felt there was a real need to expand it to a national initiative and that’s exactly what we’re doing.

There are some 12 initiatives under CNCI. Initiative Number 8 is the Education Initiative. The NICE Initiative is an outgrowth of that. We’ve inherited all the activities that are ongoing under CNCI-8 and are now expanding and building upon those activities.

The 60 day cyber review laid the foundation for a number of things that were actually implemented under the NICE initiative,
this idea of the need to build capacity for a digital nation is clearly part of our mission that we’re really taking on board as something critical not only to the national security of our nation, but for the future economic and innovative future of our systems as well.

I want to digress a moment to speak to that. I know everyone is well familiar with the threat vectors out there that are related to cyber security and how important those threats are and how important it is that we respond to them. It’s almost like you hear that as a constant refrain and it starts to have a negative psychological effect -- the sky is falling, the sky is falling -- and we tend to tune it out. So there’s another aspect that’s critically important as well.

If you think about the entire STEM enterprise -- Science, Technology, Engineering, Mathematics career fields, what’s happening in those spaces, and think about the past half century of advancements there, and try to imagine what that would look like if there were no computers, if there were no computer networks involved at all. It would be a completely different picture. And certainly as we move forward deeper into the 21st Century we’re going to see that dependency on computer networks increase and become more and more critical.

Fundamental to that, those systems have to be secure, they have to be reliable. So in a very real sense, cyber security is a fundamental enabler of the entire STEM enterprise, so we have to pay attention to that. We hope to maintain our world-class science and technology leadership and advance that into the 21st Century.

Also it really focuses on this issue of where is the next generation of U.S. citizens going to come from that are going to man those positions that we need, both within the DoD and outside, fill those really critical positions that need cyber security expertise, need security clearances. We see cyber as one of those things that you can really engage young people at an early age with hands-on experience to get them excited about going into these STEM fields. It’s one of those areas that’s computer sciences in general that allows you to not only go deep into a technical field, but also impact other areas related to that. You find computers everywhere. So most people have multiple interests and desires. It’s very easy to take a computer science background, cyber security background, and apply it to other areas of interest as well. So we’re looking
to really highlight that aspect of cyber security as a way to motivate young people to move into this area.

The President’s been very supportive of this activity, has been behind this effort a hundred percent from the beginning. I’ve got excellent connectivity with Howard Smith’s office at the White House, the Cyber Coordinator. He talks about the NICE Initiative and the NSTIC Initiative, the trusted identities in cyberspace, as the two critical components from an education/training standpoint that they’re talking about moving forward. So we really appreciate that support and continue to enjoy that type of relationship.

I guess it’s kind of good and bad. You have the attention of the White House, that’s a good thing. It’s also a bad thing. If you’re going to fall, it’s a long way to the ground from there. [Laughter]. So we’re sensitive of that and doing everything we can to make sure that we don’t fall into any traps there.

This is just giving you a little highlight of how we’re moving from CNCI-8 to this national initiative, from federal focus to national focus, not just looking at the federal employee base, but the entire population of the United States. Education and training, we’ve already heard a number of people talk about what’s happening within the Air Force. I’ve been very fortunate to already engage some of the professionals at the Air Force Laboratory doing excellent work in training of professionals within the Air Force and trying to find what kind of lessons learned we can take from that and extrapolate across the rest of the country.

Federal pipeline is simply just a piece of the national pipeline. It needs to be a broader pool that we can draw from, and we’re certainly looking to expand that pool.

The current structure of the NICE Initiative was inherited from underneath the CNCI and we’re in the process of tweaking this a little bit, but primarily this is still true today. Our first track deals with the awareness campaign that’s been led by the Department of Homeland Security. They’ve been running for the past eight years or so the October Cyber Security Awareness Month activities. Right now they’re focusing on expanding those activities so they occur not only just in October but around the calendar year. We want events to capture people’s imagination all year round.
This current year they focused primarily on the high school population and their parents since they’re already engaged in the cyberspace activities, trying to build upon that engagement and enthusiasm and move them in a direction towards cyber security professionals.

The intent is to move that focus across the demographics of the entire population so in future years you’ll see a focus on even younger groups, a focus on older groups, a focus on seniors. A focus on every component of the population.

Eventually as you all know, this is not just a national issue, it’s an international issue. We’re already fielding requests from other countries interested in what we’re doing in this space, wanting us to come and speak and talk about how we can partner together, and we’re certainly looking to do that. We want to make sure we have our own house in order first before we move out into that area, but we’re planning to do that in the future.

Track 2 deals with education. The formal education piece where we’re looking at everything, the entire spectrum, K-20+ if you will. It’s being led by the Department of Education and the National Science Foundation, two agencies that historically don’t play that well together. They have very different missions. But in this instance we’re finding remarkable cooperation and collaboration across those two agencies. Some really good work, ideas, coming out of that space. As you can imagine, NSF is intensely interested in the research component of education in general, the whole idea of STEM education and how that needs to be enhanced, how computer science needs to be more vigorously injected into the STEM fields, and then the cyber security components of that as well.

We’re looking to increase the number of teachers that have the skill set to do that type of education, particularly in the K-12 space. We understand that if you don’t capture the imagination of young people as early as 6th, 7th, 8th grade, you really start to lose them. That’s the age where you really need to bring them along.

I think all of us can look back over our educational careers and identify that one or two outstanding teachers that really pushed us into the technical direction or in a field that we wanted to go in. Wouldn’t it be great if that was the norm
as opposed to the exception of the type of teachers that you ran into in that space? So the National Science Foundation is addressing that issue, trying to increase the number of technically skilled instructors for the K-12 space.

Department of Ed, it really has the mandate to provide funding. I’ve had members from the department tell me they operate more as a bank handing out money to the states to operate in certain spaces. We don’t have the power at the federal level to dictate curriculum or standards of what’s happening across the states. It’s really 50 different experiments that are going on. But we can do things to encourage and help push people along into the right direction. Activities like the Race to the Top, we’ve been considering adding cyber security components to that competition so that states are involved in competing for Race to the Top dollars, and they have cyber security programs in there to give them a leg up in that area as well.

Part of this whole effort, too, if you will, there are lots of activities that are already ongoing. Not only state, local, tribal governments, private sector industries, for profit, non-for profits, associations that are doing things in the training and education space. There’s a real need to get all that information together, form a repository, and make it widely available so people know what’s already out there, what’s already available on the ground. A certain baselining, which we’re planning to do across all four of these component areas of the program.

Once we have a really firm idea of what’s happening already, we’ll be able to do gap analysis, resource analysis, see where things are missing, design programs to meet those missing needs, maybe suggest ways to redistribute the limited resources that are available to have a better coverage, and then to actually build and propose new programs that would sit on top of those that would accomplish things that none of these agencies or institutions or companies can do by themselves. We’re all about the collaboration, the public/private partnerships and achieving more than we can separately. So that’s the overall goal, where we’re going with all of this.

The federal cyber workforce structure has already been alluded to. It’s a very complex field. It’s a dynamic field, it’s changing. It’s not that there’s one title out here, you’re a cyber security professional and everybody in the whole federal
government, private sector, all fall under that one description. There have been a number of studies. DoD has presented a study. The Federal CIO Council, Office of Personnel Management, have all done significant studies over the last two years trying to get a handle on exactly what does it mean to be a cyber security professional? How many different job titles are there? What are the required training certifications, education requirements for each of the different titles? So for the first time under the NICE Initiative we’re going to bring all those studies together, bring the principal supporters of those studies, the people who actually did the work, and see where the commonality is across that space, try and remove some of the confusion that exists out there across federal government as to what’s actually happening there and come out with one message, one voice, one document that’s going to represent what we really mean.

I’ve seen studies that have talked about as many as 19 different career fields identified as part of the cyber security workforce, or as few as 11. Probably the right number is somewhere in between and we’re certainly not looking to come up with a one-size-fits-all. There’s going to be different flavors for different types of organizations and we’re going to try to articulate that entire process. I think that will move us forward. Certainly federal contractors will want to align themselves with that so they’ll have an easy flow in and out of the system. We know that in the private sector they face the same type of challenges with their workforce. Some are probably ahead of the federal government. We’re looking to open these two-way communications so we can learn from them what they have done and we can share our best practices back in the other direction as well. Certainly a huge number of small to medium sized companies don’t even understand yet that they have a real need to do training and development within the cyber security space.

They will learn. As new systems are coming down the pike, ideas, for example, the SmartGrid is going to affect everybody in the country. There are some 3200 private utility companies across the country which will all need training in the operations of their SmartGrid systems and not to mention the end users which is everybody in the country, what it means to have these systems in your house and how they will operate. So lots of work to be done there.

Office of Personnel Management is really going to lead up the federal cyber workforce issue, but this is bigger than that.
We’re going to have a component that looks at state, local, tribal governments, the non-federal government aspects of it. We’re going to have another component that looks at the private sector as well, led by other agencies within that track. So we can really get a comprehensive picture of what’s happening within the workforce structure.

Closely related to that, our last component area dealing with workforce training and professional development. As already was mentioned by the last speaker, there’s lots of training already ongoing, very good training ongoing. A key factor with that training is it must remain dynamic. It must be refreshed often. We must keep pace with what’s happening in the field, close ties to the R&D community that are generating the new ideas and the new concepts, as well as the threat vectors and vulnerabilities out there. All of that needs to be addressed as we move forward.

So the plans that are being put together call for constant refresh, they call for more hands-on training, and those four categories underneath that kind of look at the different types. That’s a rough breakdown of the different types of individuals that we’re looking to affect. General IT users. Virtually anybody in federal government, any office you walk into there’s a computer on their desks and it’s connected to some other computer somewhere else. So they need to be aware of what’s going on in that space.

Then you have the IT infrastructure protection, your SysAdmin folks, your cyber security professionals defending those systems. There’s a whole other component that deals with law enforcement, counterintelligence, and then also special operations headed out of the National Security Agency. That is the only still classified part of this program. Everything else has been declassified.

Both DoD, Office of Director of National Intelligence, and DHS are tri-leads of this area. They’re working closely with the Track 3 folks to make sure that we marry up what’s happening in the workforce structure with the training and professional development needs. More than just training, you have to worry about career paths. What does it mean to come in and be a cyber professional? Do you have a clear-cut career path? Do you know what your next training step’s going to be? This idea of being able to cross-train across domains which I heard mentioned earlier is also an excellent idea to get a broadening of the
training experience. And it’s very well needed within this field. You need to be able to look at problems from multiple different directions to really get a good handle on what’s happening there.

Here are some of the achievements that have been listed under the previous CNCI-8 that we’re building on. I’m not going to read these. I’d just mention a couple of things.

The Centers of Academic Excellence Information Assurance Education is a program that’s been run for some time now by NSA and the Department of Homeland Security. Currently some 127 institutions across the country have received this designation. Just this past summer we brought into the fold the first group of community colleges. Community colleges have a key role to play as we’re going through these economic times and we’re having a lot of adults going back to school for retraining, reeducation in space, they’re going to go to community colleges because of their ease of access. So we’re looking to expand the number of community colleges in this realm, have at least one in every state.

There also is a tie-in to the Federal Cyber Service Scholarship for Service Program that’s run out of the National Science Foundation. This program has been around for about ten years. I had the privilege to be a program manager for that back in the early 2002-2004 timeframe. It’s generated close to a thousand graduates at this point, some 80 percent of them have gone to work for the National Security Agency. Really high-class, top tier professionals being generated out of that program. Some of the legislation that’s been bounding around the Hill the last year or so is looking to really plus-up that program significantly.

So there’s good news in this space. Lots of good things happening. The things that we’re planning to do in the NICE Initiative is to build on all those good things to make sure we understand what’s happening, what’s working, define metrics, baseline where we are now, and really carve a solid path forward.

So this is just where we are, and [NIST], has been designated as the lead agency for this multi-agency effort. You saw all those other agencies that are involved. [NIST] has a reputation as being a neutral arbiter, if you will. We’re very heavily involved in standards, international and national
standards, and we’re going to use that role to enhance what we’re doing across the space and bring everybody together.

This pipeline chart speaks to the digital nation outcomes that are right there in green. The research professionals, the researchers, the next generation of people who will be teaching at the college level and the K-12 level, how all of this feeds into that process, all the way down to just the aware citizens who are really looking to touch everybody in that space and to accelerate and expand the pool and the number of people that exist across that space.

Our [inaudible] being led by Homeland Security, Tim Frasier’s doing an excellent job over there. He’s getting ready to rotate out. He’ll have another person step into those roles. Our leads from Department of Ed and Science Foundation for the formal education track. Also the workforce structure, Maurine Higgins at OPM. We’re actually going through some transition with this particular track to go the three kind of sub-components of that area, make sure we get that aligned properly and cover more than just the federal government piece.

The last piece, the workforce training, professional development, really a big set of activities going on. They have a number of activities including things like the VTE, virtual training environment is geared up to be able to simultaneously touch some 125,000 federal employees at the same time; a platform prepared to deliver cyber security content. We’re looking at how we train to the annual requirements with all federal employees to go through cyber security awareness training. We think it can be improved greatly. It’s really pretty much a check the box kind of exercise at most agencies. We want to change that to more hands-on, maybe something that you only get 15 minutes of every month or so, things that will actually stick with you and not something that just is a paper exercise, so we’re looking to be effective in that space as well.

I know I’m the last person here between you and the end, so I wanted to leave plenty of time for questions and leave my contact information up there for any future endeavors.

**Moderator:** Thank you, Dr. McDuffie, we very much appreciate it. I have a number of questions, and a lot of them are similar.
First of all, what kind of funding profile do you have? Do you have the funding you need to be able to accept this broader mission? Can you give me an idea what it would be in the out-years?

**Dr. McDuffie:** Two things I need to do first. First, in your introduction at the beginning you listed my current job title as Associated Director of the --

**Moderator:** Right.

**Dr. McDuffie:** That was actually my previous job. I didn’t want people to think I was still moonlighting over there for those guys. That was a great job, though.

The funding issue’s pretty tricky. The funding lines that existed under CNCI still exist. Those funding lines are ongoing. Some additional funding was identified to stand up this coordination piece, the program management piece at NISTA and some of the other agencies that hadn’t been playing.

We did pretty well in our FY12 bid to get additional funding. It looks like that’s going to come out all right.

Of course the CR has complicated everything. Actually moving funding from the intelligence community under the CNCI to NIST has proven to be a challenge in itself. The agencies don’t really talk well. The lawyers have gotten involved. It’s been kind of a nightmare. So we’re still struggling with that. But we think as soon as we get past this hurdle, we’re funded adequately now to at least get off the ground with what we’re trying to do here. Certainly to do big projects, you talk about public service campaigns. To really do that well you really need hundreds of millions of dollars, and nobody’s expecting in this environment for that kind of money to flow to a program like this. This is why we’re really focused on these public/private partnerships where we engage with the private sector.

I’ve got a venture capitalist group out in Northern California that’s very interested in bringing funding to the table. Things that are going to be sustainable and be external to the federal budget process so that they will -- This is going to be an ongoing effort. This is something that will be with us as long as there’s cyberspace, which is forever. So we’re really looking at ways to have it funded sustainably without
having major impacts on the federal budget.

**Moderator:** Not to press you, but is there a number associated with adequate funding?

**Dr. McDuffie:** There’s a number. I don’t know if I can say -- Adequate is a tricky word.

**Moderator:** That was your word. [Laughter].

**Dr. McDuffie:** The funding level for FY10, and this is just the unclassified piece, was probably around the $20 million, and that covered a lot of activity. So that’s all we really know for sure. Everything else is kind of still up in the air with what’s happening.

**Moderator:** I have a number of questions on one slide you had, you were concentrating on above K-12 into college. A number of questions and you addressed them, I think, in your verbal remarks. But in terms of what are you doing below K-12 and all the way down to where the 4th and 5th grade level where some of this stuff needs to be taught.

**Dr. McDuffie:** Oh, yeah. There are a number of competitions. At the college level they’re having these camps over the summer where they’re having challenges, defend the flag kind of challenges. They were being very successful and people wanted to expand that to the K-12 level and thought that the skill set really wasn’t there, K-12, to do that. Then they tried to do it and found out that the skill set actually was there, and they’ve had some very successful high school summer camps that are doing that as well.

We’re also looking to engage the younger people in contests, these PCA contests. You’ll see on the DHS web site right now some YouTube like videos that young people have put together themselves. The ones that win that competition wind up getting recognition and will be used as part of the campaign.

Out at the Naval Post Graduate School there are some faculty members that have been working on cyber security games that are really teaching tools that are very attractive to the younger demographic that we’re looking to push out as well. So even we’ve got the Girl Scouts and Boy Scouts involved in doing things like merit badges for cyber security.
Moderator: Have you gotten close to a standard curriculum in any of these areas?

Dr. McDuffie: that’s interesting. The CAE program actually does have standards for curriculum that they put out, that schools have to meet in order to become one of those certified centers. It’s much more difficult at the K-12 level. The first challenge is really to get meaningful computer science training in that space and then kind of sprinkle the cyber security pieces in across that area. All the curriculums at the K-12 level are already very full, so we’re not necessarily advocating whole new courses. Better yet would be modules that can be used across the courses that are already there. We’re working on standards to that, but we haven’t gotten it completely ready yet.

Moderator: I know it’s tough with a new program like this, but are there other countries that are doing this well that we can steal ideas from? If so, which ones come to mind?

Dr. McDuffie: I haven’t heard, seen any examples of other countries that are really kind of ahead of us in terms of the sophistication, of the need, of recognizing the need to do this additional training.

It’s been said that the country that trains and educates best will win in the 21st Century, and I certainly am a firm believer that the United States is still the lead in terms of the best education system in the world. We’re certainly being challenged and pushed hard by China, India, other places, the European Union. There are activities going on there. But because it’s so new, I don’t think anybody’s ahead of us yet in that space, in that regard.

Moderator: I might note that my last year on active duty I was the President of National Defense University, and I traveled all through China to see what the Peoples Liberation Army was doing. They told me that the Army alone was producing more scientists and engineers than the entire United States.

Dr. McDuffie: Absolutely. The numbers game is amazing. If you start to look deeper inside of it, there’s a lot of question about the quality of the types of degrees that are being generated out there. Certainly we’d never be able to win the numbers game, just because of the population difference, but I think quality wise we’re still well ahead.
Moderator: We had a speaker earlier, I think it was yesterday, that noted that the half-life of education, certainly at the collegiate level, is not measured in decades. By that she meant that you get a baseline, in most fields you get a baseline in physics or any kind of science, and that will carry you through higher levels. But in this area she noted that your half-life -- you mentioned a year-long set of trainings. It seems to many that you’d have to do this quite a bit more often than --

Dr. McDuffie: Absolutely. That’s one of the biggest challenges. Not only with cyber security but computer science in general. I spent seven years at Florida State University as a faculty member and fully 50 percent of my time was spent just trying to stay current. The field moves so quickly, you really have to spend a lot of time trying to stay current with that. And academic institutions traditionally do not move that quickly. There’s a joke about how do you change a department? It’s as one professor dies at a time. That’s the only way you can change it. In some sense that’s really true.

So the challenge, and what we’re seeing in those schools of academic excellence, the ones that are really doing it right, have dedicated faculty members that are well aware that they need to stay mobile and up to date and current. They’re kind of instituting this teaching school environment just as you see in the medical field, where you’ll have practitioners where they’re actually doing the real work. University of Tulsa [inaudible] comes to mind where they actually have CERT capabilities there. They have labs, they’re well connected with the U.S. environment, the government environment, and the research activities. So their students get actual hands-on experience of what’s happening in the field right now. We think that’s an excellent model.

Moderator: Dr. McDuffie, thank you very much for an enlightening presentation. On behalf of all of us at the Air Force Association, thank you for your service and your time today.

Dr. McDuffie: Absolutely. Thank you.

# # #